(1)

Technical Report for the Cargo Movement Operations System (CMOS)

Security Plan, (Updated)

16 JULY 1990

Prepared under

Contract Number F11624-88-D-0001/6K12
CDRL A004-22-01

Prepared for

Standard Systems Center (SSC)
Deputy Chief of Staff for Acquisition
Cargo Movement Operations System Division
Gunter AFB, AL 36114

Prepared by

Science Applications International Corporation (SAIC)
6 Eagle Center, Suite 2,
O'Fallon, IL 62269

Table of Contents

SECTION I.

INTRODUCTION. The purpose of this Technical Report is to provide the CMOS Program Office with an updated version of the CMOS Security Plan. This enhanced document contains all recommended changes provided by the Government and is assigned CDRL Number A004-22-01.

SUMMARY. Not Used.

CONCLUSION. Not Used.

SECTION II.

RESULTS.

The updated version of the CMOS Security Plan is provided as follows:

SECURITY PLAN

For

CARGO MOVEMENT OPERATIONS SYSTEM (CMOS)

16 July 1990

Standard Systems Center
Deputy Chief of Staff for Acquisition
Cargo Movement Operations System Division

This Cargo Movement Operations System (CMOS) Security Plan is developed in accordance with AFR 205-16 and SSCR 205-1. The plan will document the relevant security requirements of CMOS.

1. GENERAL INFORMATION.

CMOS is a top down directed program (DEPSECDEF memo, 7 Sep 84) that automates base-level transportation at 240 sites worldwide. Air Force Program Management Directive (PMD) #5272(2)/38610F, Cargo Movement Operations System (CMOS), 5 Dec 86, as revised 21 June 1988, directs the development of an automated system to support regular and crisis cargo and personnel processing, documentation, movement, and tracking. The CMOS Program will be produced according to Air Force 800-series and other related regulations.

The following are applicable documents:

AFR 205-1, Information Security Program.

AFR 205-16, Computer Security Policy.

CSC-STD-001-85, Department of Defense Trusted Computer System Evaluation Criteria.

CSC-STD-002-85, Password Management Guidelines.

CSC-STD-003-85, Computer Security Requirements.

CSC-STD-004-85, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements.

DOD Directive 5200.28, Security Requirements of Automated Information Systems (AIS).

2. SCOPE AND APPLICABILITY.

The Air Force has defined (1) the user requirements to be automated in Increment I and (2) the user requirements to be automated in Increment II. Increment III actions have not been initiated. Increment I provides automation of base-level traffic management which includes the preparation and reporting of cargo movement. Increment II adds war fighting capabilities for movement visibility, contingency planning, mobility execution, and force deployment. Increment III will be the vehicle for adding pre-planned product improvement.

CMOS will be implemented via a distributed processing hardware configuration. (See Figure 1-1.) A UNIX-based AT&T 3B2/600G minicomputer will be used to provide the external communications functions and the maintenance of the central integrated database. It will also provide the control over the CMOS Local Area Network (LAN). Another UNIX-based AT&T 3B2/600G minicomputer will be used by the CMOS System Manager to perform such duties as database administration and system restart and recovery. This additional processor will also serve as the backup processor to the primary processor. The primary and backup processors will have access to the Defense Data Network (DDN) for use in external communications. Intelligent personal computers will provide the user the functionality needed by the TMO work areas. The PC Workstations will communicate with the primary and backup processors and each other via the LAN (direct coupling or terminal servers). The last set of hardware that is part of the CMOS configuration is the LOGMARS equipment. This suite of equipment consists of hand-held terminals and LASER scanning devices. This equipment will be used by the transportation personnel to enhance the inbound and outbound cargo processing functions.

3. OBJECTIVES

The overall objective of this plan is to establish a CMOS security program. The following paragraphs identify the major program phases and the security actions required for each of these phases.

Conceptual Phase -- The System Segment Specifications for Increments I and II distinguish the required operational capabilities, functions, and features. Relevant security requirements will be included in the Increment I requirements documents. In addition to identifying these requirements, a preliminary risk analysis will be performed. This risk analysis will examine known threats, available security countermeasures, and anticipated operational vulnerabilities. The preliminary risk analysis will become a key component of the functional baseline.

Production Phase -- During the production phase, the risk analysis will be updated to include those design efforts that will contribute to meeting all security requirements. Following this analysis, an update and re-publication of the risk analysis will take place.

Deployment Phase -- A final published risk analysis will accompany CMOS Increment I when it is deployed. Included in this deployment package will be a written certification of security measures by SSC/CC or his designated representative. MAJCOMs will update this document to reflect threats and vulnerabilities of their respective operational environment.

Life-Cycle Support Phase -- The Increment I Risk Analysis will be updated prior to Increment II IOC. In addition, major changes driven by Increment III task orders will require an update to the risk analysis. Otherwise, updates will be required every three years.

4. RESPONSIBILITIES ASSIGNED

The Standard Systems Center is responsible for CMOS development. The system will be contractually developed under a firm fixed price contract. Program Management will be provided by the CMOS Program Office, SSC/AQFT.

5. SECURITY PLANNING GUIDANCE

CMOS will process sensitive unclassified information. The CMOS development contractor will review with the Program Office all security related requirements and specifications.

During design reviews (System Requirements Review, System Design Review, Preliminary Design Review, and Critical Design Review), MAJCOM representatives will be invited and encouraged to attend so that the operational users, or Designated Approving Authority organizations, will be kept abreast of all information and decisions concerning security tradeoffs, revised requirements, etc.

6. RISK ANALYSIS GUIDANCE.

The risk analysis is the foundation for documenting system security. The analysis should:

(a) Identify the resources to be protected.

(b) Determine the threats against the resources.

(c) Determine the vulnerabilities of the system.

(d) Determine whether safeguards will lower the risk.

(e) Designate the certification authority and document the criteria that must be met to obtain a C2 level of trust by 1992.

It is a DOD requirement that all automated information systems, such as CMOS, which process sensitive unclassified information, are secure to at least level C2 by 1992. The ways in which this requirement is met must be documented in the risk analysis. An Increment III Task Order is being developed with award to the development contractor on or about 1 December 1990. A requirement is being built into this task order that will provide for full C2 in CMOS. This includes discretionary access control, object reuse protection, user identification and authentication, and system security audit features for the information processed by CMOS, consistent with current directives and policy. This Task Order will also ensure training for both the user and the system administrator on all C2 requirements.

7. SECURITY TEST AND EVALUATION (ST&E).

ST&E serves to test security measures and to validate the assumptions about the effectiveness of existing safeguards and what is needed to improve these safeguards. The results of ST&E may reveal the need to revise and repeat parts of one or more steps in the risk analysis. The following will encompass the steps of the CMOS ST&E efforts:

(a) Determine the Objective.

(b) State the Assumptions.

(c) Describe the Constraints.

(d) Determine the Test Procedures.

(e) Execute the Tests, Analyze the Results, and Produce the Report.

8. SCHEDULE.

Confirmation that CMOS meets all criteria for C2 level of trust is the responsibility of SSC/CC or his designated representative. The CMOS Program Office will provide recommendations and other necessary assistance to ensure the timely completion of this certification process. CMOS Increment I is scheduled for IOC in February 1991. The Final Risk Analysis for CMOS Increment I will be completed prior to IOC.

9. SUMMARY

The purpose of this plan is to document the relevant security requirements of CMOS. The tenets of the Security Plan will be adhered to throughout the CMOS life cycle.